Chapter 3

AN ATTACK-FAULT TREE ANALYSIS OF A MOVABLE RAILROAD BRIDGE

Matthew Jablonski, Yongxin Wang, Chaitanya Yavvari, Zezhou Wang, Xiang Liu, Keith Holt and Duminda Wijesekera

Abstract Mechanical and electrical components of movable bridges are engineered to move heavy concrete and steel structures in order to allow water traffic and rail and/or vehicular traffic to pass many times a day despite harsh weather conditions, storm surges and earthquakes. The bridge spans must also support varying rail and/or vehicular traffic loads.

This chapter considers known and theoretical risks posed by movable bridge system attacks and faults in a single stochastic model based on attack-fault trees. Risks associated with railroad swing bridges are presented, along with the attack-fault tree model and the analysis results.

Keywords: Cyber-physical systems, movable bridges, attack-fault tree analysis

1. Introduction

Movable bridges constructed over waterways are specifically designed to allow traffic flows on and over waterways. Most movable bridges, which are called "heavy movable structures," maneuver many tons of steel and concrete under the control of modern controllers even under difficult weather conditions.

Bridges have been targets of attacks since ancient times. From castle drawbridges to supply line bridges in Europe during World War II, pitched battles have been fought over bridges. In this post-Stuxnet era, new risks are posed by attacks on programmable logic controllers and networked industrial control systems – the cyber-physical components that control movable bridges. Consequently, securing a modern movable bridge requires the consideration of faults in the physical, mechanical and control aspects of the bridge as well as the cyber security of electro-mechanical components that actuate the movements of physical components.



Figure 1. An open BNSF railroad swing bridge [18].

Faults and vulnerabilities in a system are typically studied by collecting and analyzing data about failure modes. Design corrections are then instituted and the resulting reports are shared with the community to mitigate hazards and risks. Unfortunately, a repository of reports pertaining to movable bridges does not exist for three reasons. First, although they may share some common components, no two movable bridge systems are built the same and operate under the same environmental conditions. Second, the faults and the methods for handling outages vary, but this information is not recorded in a centralized public repository. Third, no cyber attacks have as yet been reported against movable bridges, although attacks against other control systems could be repurposed to target similar components in movable bridges. To address the lack of data, this chapter models the impacts of failures on movable bridges with a focus on railroad swing bridges (Figure 1).

A literature review indicates that intentional attacks and accidental faults cause movable bridge failures; therefore, a comprehensive model of attacks and faults that result in failures is needed. This work employs the combined attack-fault tree model of Kumar and Stoelinga [16]. This model was built on previous work on attack trees and fault trees to support qualitative and quantitative analyses of combined system security and safety properties. The model is leveraged to create an attack-fault tree for a swing bridge, following which each node in the model is translated to a stochastic timed automaton used by the UPPAAL Statistical Model Checker [7]. A qualitative analysis of the attack-fault tree can be used to identify the root causes of swing bridge system failures whereas a quantitative analysis allows for the incorporation of likelihood values, costs and impacts of disruptions; these two types of analyses are important components of a risk analysis. The utility of the attack-fault tree model in movable swing bridge risk assessments is also discussed.

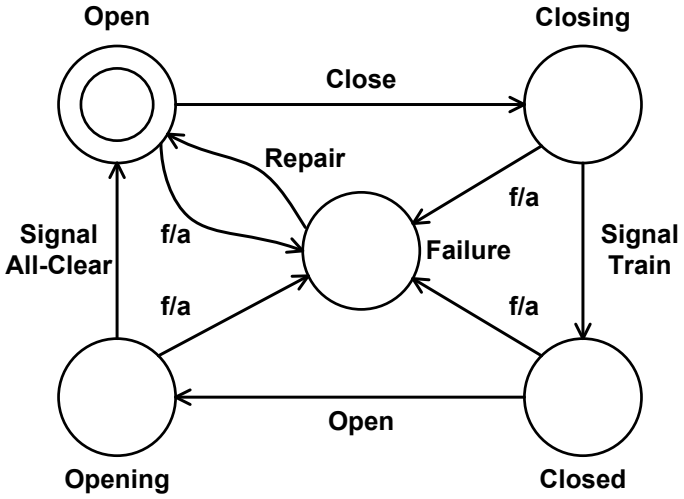


Figure 2. Finite-state machine model of a movable bridge.

This research has two main contributions. The first contribution is a thorough security and safety analysis of a movable swing bridge using an attack-fault tree model. Although the focus is on cyber attacks, physical attacks are also considered because bridges, by their very nature, have open physical access. The second contribution is the application of the attack-fault tree model to a real-world system.

2. Functionality and Failures

This section presents a model of swing bridge functionality and potential system failures. The discussion clarifies the risks of attacks and faults that impact railroad swing bridge operations.

2.1 Functionality Model and Usage Scenarios

A swing bridge is considered to be open when the bridge is rotated parallel to the navigable water traffic direction, enabling water traffic to flow and halting overland traffic. The bridge is considered to be closed when it is aligned with the overland tracks, halting water traffic while enabling overland traffic to flow. These operational states and their transitions are modeled as a finite-state machine shown in Figure 2. It is assumed that a railroad swing bridge is open by default to favor water traffic, and is closed when needed to accommodate passing trains.

When a bridge in the open state needs to transition to the closed state, an operator signals a close request to the bridge control system. At this point, marine craft are alerted via radio, lighting and/or alarms and given time to steer clear of the bridge. Gates may be lowered to prevent the flow of overland traffic. The control system also checks overland traffic control sensors to avoid

unsafe operations. After all the sensor checks are completed, the drive system mechanically walks the pinions around the curved rack, rotating the pivot pier and bridge span 90 degrees. End lifts are then secured, wedges are pushed into place (in the case of center bearing systems), the centering device is engaged and the track is locked on both ends of the bridge [15].

The bridge is now closed, and lights and signals are used to inform operators to permit overland traffic to flow. After overland traffic has passed over the bridge for some time, the process is reversed to move the bridge back to the default open state.

The functional use cases of a swing bridge are modeled as a Moore finite state machine with four states – open, closing, closed and opening – as shown in Figure 2. Failure states are introduced when the bridge is in these states or transitioning between the states.

2.2 Classification of Failures

A movable swing bridge is a "binary dynamic and repairable system" [5]. It is binary because its failures are modeled using Boolean variables, dynamic because the order of component failures impacts the system failures and repairable because faulty, degraded and failed components can be replaced. According to this classification, a swing bridge may also be in a failure state, which is defined as a stopped and dysfunctional state, where it remains for a period of period until repairs have occurred and normal functionality can resume. If the bridge fails in the open or closed states, then the passage of overland or water traffic, respectively, is halted.

3. Attack-Fault Tree for a Movable Swing Bridge

Attacks and faults can result in failure states. The swing bridge attack-fault tree segments in Figures 3 and 4 show both types of failures in a single model. As a top-down failure analysis formalism, an attack-fault tree is a directed acyclic graph that analyzes the top-level safety or security goal and refines it into smaller sub-goals. In the case of the bridge model, the top-level goal [G_0] is "prevent bridge movement," which corresponds to the definition of failure.

An attack-fault tree comprises gates and leaves. Figure 5 shows the five standard, dynamic fault tree gates: (i) AND. (ii) OR; (iii) FDEP (functional dependency); (iv) SAND (sequential AND); and (v) SPARE (spare inputs). The leaves in an attack-fault tree are either basic attack steps or basic component failures, corresponding to attacks and faults, respectively. The leaves are represented as stochastic timed automata (described later in this chapter). Interested readers are referred to [16] for details about attack-fault trees and their use in quantitative security and safety analyses.

It is assumed that a generic swing bridge uses programmable logic controllers for control automation; wireless networks and manual overrides for interconnections and operator control, respectively; an AC-powered electric motor and

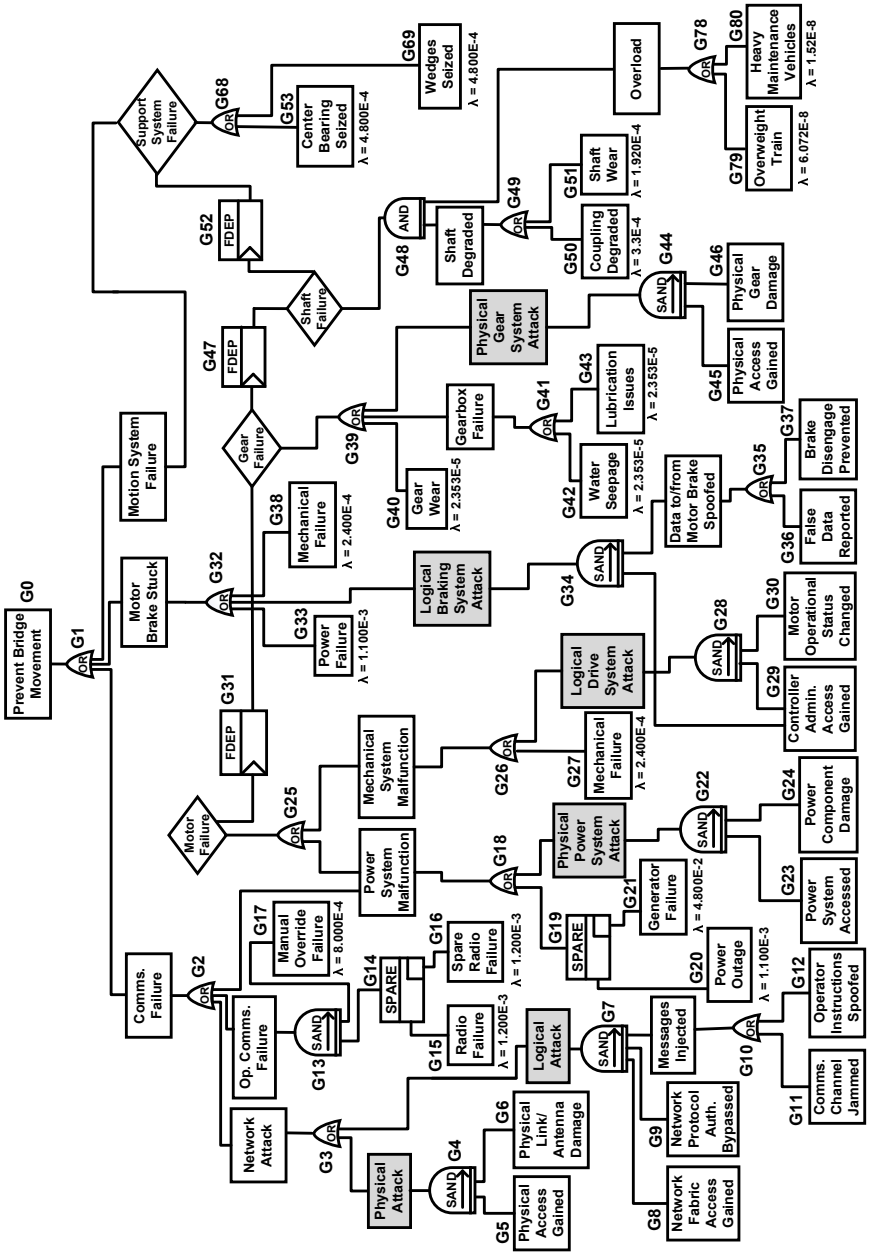


Figure 3. Attack-fault tree for the mechanical and electrical subsystems.

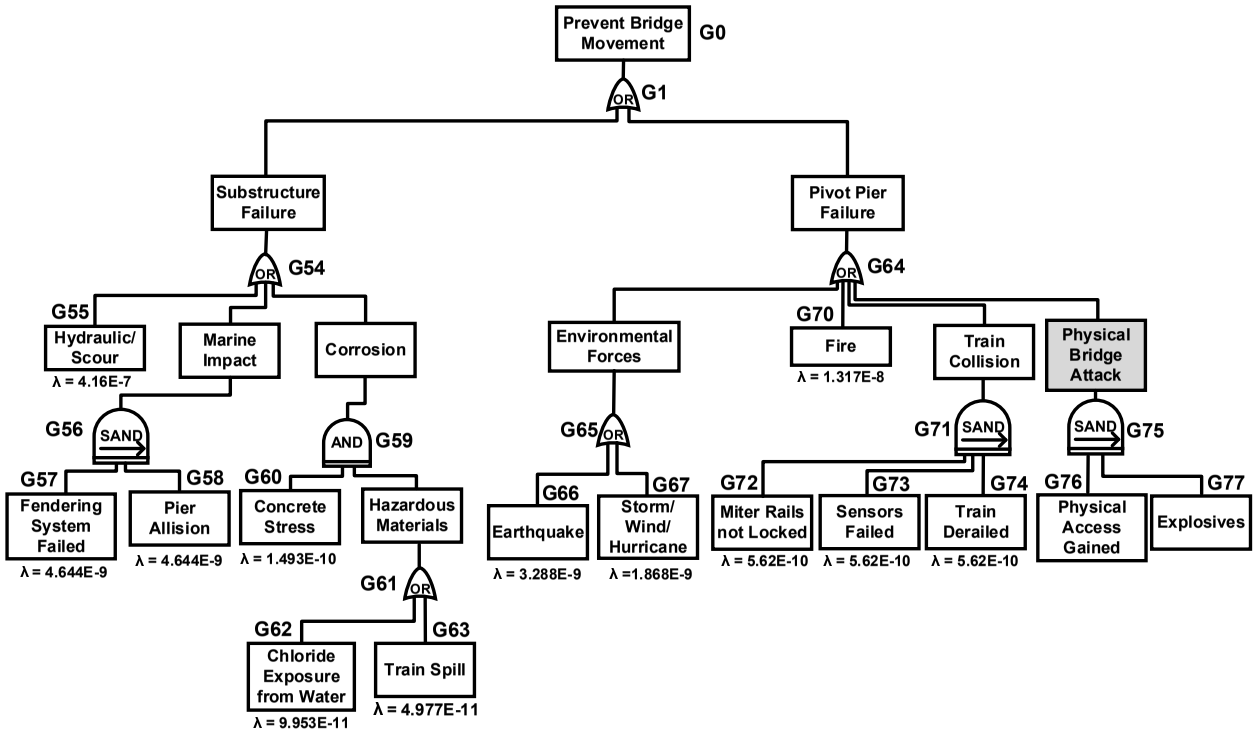


Figure 4. Attack-fault tree for the superstructure and substructure subsystems.

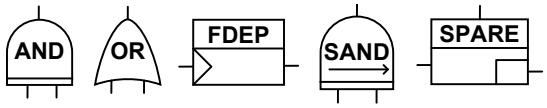


Figure 5. Attack-fault tree gates.

motor brake; a simple mechanical miter rail system that does not require separate electronic controls; and modern power systems.

Attacks or faults can take any one of the following five paths to realize the top-level goal $[G_0]$:

- **$[G_2]$:** Communications failures prevent local or remote operators from moving the bridge.
- **$[G_{32}]$:** Stuck electric motor brake prevents bridge movement.
- **$[G_{68}]$:** Support system failure prevents the motion system from functioning.
- **$[G_{54}]$:** Substructure failure causes a major bridge outage.
- **$[G_{64}]$:** Pivot pier failure causes a major bridge outage.

Figure 3 shows paths $[G_2]$, $[G_{32}]$ and $[G_{68}]$. Figure 4 shows paths $[G_{54}]$ and $[G_{64}]$. All five paths could result in $[G_0]$.

4. Movable Swing Bridge Components

This section describes the basic components and subsystems of a movable swing bridge [15]. An overview of swing bridge subsystems is provided in order to discuss the attacks and faults in the attack-fault tree. Certain basic attack steps and basic component failures are highlighted during the discussion. Note that swing bridges are falling out of style in favor of lift bridges because their central piers cut waterways in half, which can prevent the passage of large ships.

4.1 Superstructure and Substructure

A swing bridge superstructure consists of a pivot pier $[G_{64}]$, which is centered in a navigable water channel (Figure 1). The pivot pier is typically fixed in the middle of the rotating span, enabling it to remain balanced as it rotates. Fires $[G_{70}]$, vehicular collisions $[G_{74}]$ and environmental forces $[G_{66}, G_{67}]$ are some of the primary causes of failures in a bridge superstructure system [6]. Additionally, between World War I and the Vietnam War, bridge destruction $[G_{76}, G_{77}]$ was an effective measure used by local populations to limit large armed force movements into their territories [10].

A swing bridge substructure $[G_{54}]$, which includes the foundation for the pivot pier (a round or square concrete base that vertically stretches above

the water line), is designed to withstand horizontal loads and keep the bridge centered. Hydraulics issues, such as bridge scour [G_{55}] resulting from water scooping out the soil and sediment that support the bridge pier, caused 60% of complete bridge failures in the United States between 1950 and 1990 [6]. A timber or crib fendering system [G_{57}] is often installed to prevent ships from striking the center pier or to guide them away from the pier. Allisions [G_{58}] that result from marine vessels striking the pier base are the second greatest risk to the substructure and foundation of the bridge [6]. Concrete stress [G_{60}] causes cracks that could be further weakened by chloride from sea water [G_{62}] or by spills [G_{63}].

4.2 Mechanical and Electrical Systems

This subsection describes the mechanical and electrical systems that work together in modern swing bridge systems to control bridge movement. Potential attacks and faults are also identified.

Support Systems. Modern swing bridges use mechanical bearing designs from the mid-nineteenth century, such as the center bearing, rim bearing and combined bearing designs. This research focuses on bearing systems because they are the most common. A system that uses a center bearing [G_{53}] has a circular disk with a convex spherical surface fixed to the bottom of the pivot pier, which supports the weight of the bridge while sitting on top of a fixed convex disk on which the bridge rotates. When the bridge is rotated on top of the disk, it moves along a circular track around the inside base of the pivot pier that distributes the weight and balances the structure when the bridge turns; this requires regular lubrication. Wedges [G_{69}] or some other support system are used to prop up the bridge when supporting live traffic loads; these often require additional electro-mechanical components.

Drive Systems. The support system is rotated using a drive system [G_{52}, $FDEP$], which is engineered to reduce friction, limit the impact of resistance during movement and reduce the amount of torque output generated by the motor. A shaft [G_{50}] is used to connect the support system to the drive system; it is generally connected to the rack and pinion system via a grid-type coupler [G_{50}]. Additional force on the bridge span caused by overweight vehicles could result in damage to a worn shaft or rack and pinion system [G_{79}, G_{80}]. Gear drives [G_{40}] may have open or enclosed gearing for rotating the shaft [$G_{47}, FDEP$]. Possible gearbox faults are water seepage [G_{42}] and poor lubrication [G_{43}]. The drive system [$G_{31}, FDEP$] is powered by an electric motor [G_{27}] that produces the torque needed to drive the system. Motor brakes [G_{32}, G_{38}] are spring set and electrically released.

The electric motor and electric brakes, which connect mechanical and electric components [G_{18}, G_{33}] in the bridge system, could be exploited via logical or physical attacks [G_{29}, G_{30}, G_{36}, G_{37}]. The electrical drive control system in a modern movable bridge is designed to handle the sequencing of all the moving

components to ensure proper bridge control. Programmable logic controllers (PLCs) are connected to a control network that gives local and/or remote operators the ability to instruct the bridge to open or close. Each electric motor typically has a dedicated drive controller that controls variables such as speed and torque for bridge rotation. The sequencing involves instructing the networked drive controllers used to manage the electric motor(s) and motor brake(s), controlling the bridge lighting and instructing interlocking system actuators.

Local operators may open and close the bridge using radios $[G_{15}, G_{16}]$ or a control panel $[G_{17}]$ in the bridge operator's house, which is generally located in the middle of the swing bridge span. Remote network access is typically provided via a wide-area network to a back office controlled by the transportation authority. A bridge without remote access is considered to be in "dark territory." Networked components $[G_2]$ in the bridge system could be attacked logically $[G_8, G_9, G_{11}, G_{12}]$ or physically $[G_5, G_6]$ and should, therefore, be carefully designed and installed with security in mind.

Interlocking Systems. The rotational movement requires a separate interlocking system that aligns the swing span with the connecting spans in order to fully close the bridge. The interlocking system has three functions: (i) ensure that the opening bridge does not become unbalanced and remains stable; (ii) ensure that the closed bridge does not become unbalanced due to a live load; and (iii) center the bridge and ensure that it does not over-rotate. The first two functions are performed by an end lift system, which relieves the dynamic stresses caused when the bridge begins to move and helps withstand the static stresses caused by passing traffic when the bridge is closed. The third function is performed by centering devices that ensure that the bridge does not over-rotate in the horizontal plane.

After the bridge is in the proper horizontal position, the railroad tracks are closed to enable a train to pass. Miter rails are most commonly used to lock the tracks; they are lowered at the end of each side of the span via a joint when the bridge is being locked into place and they are lifted when the bridge begins to open. Depending on the bridge design, the interlocking system may have electrical requirements similar to the drive control system.

Electrical Power System. Modern movable bridges are controlled by solid-state electrical power systems that incorporate silicon-controlled rectifier (SCR) technology made up of power distribution panels, switches, circuit breakers, fuses, ground fault relays, over-current protection relays, cabling, etc. Specialized submarine cables run underwater to the center pier to bring power to the operator's house located in the swing span. Modern bridges use AC and DC motors. Due to their complexity, power systems have the highest failure rates $[G_{20}]$ of any swing bridge system [11]. Consequently, the American Railway Engineering and Maintenance-of-Way Association (AREMA) mandates an emergency auxiliary power supply such as a generator $[G_{21}]$.

5. Quantitative Analysis Methodology

The quantitative analysis employed the UPPAAL Statistical Model Checker (64-bit v4.1.19) [7] to transform the leaves of the attack-fault tree to stochastic automata that simulate failures [16]. This section describes the automaton parameters for the basic attack steps (BAS) and basic component failures (BCF) used in the simulation.

5.1 Attack Leaf Automata

Each basic attack step leaf in an attack chain is modeled as a stochastic timed automaton. When an attack is activated, the attacker waits until (s)he is able to afford a cost f to proceed. After the attacker proceeds, the attack is undetected with probability $w_1/(w_1+w_2)$ or detected with probability $w_2/(w_1+w_2)$. The attack stops if it is detected; otherwise, the attack is either ongoing or activated. An ongoing attack is detected over time with an exponential probability rate λ_1 at a cost v per day to the attacker. An activated attack is detected over time with an exponential probability rate λ at a cost v per day to the attacker.

After an attack is executed, it succeeds with probability $p/(p+q)$ and causes damage d to the bridge or the attack fails with probability $q/(p+q)$. These probabilities are based on the attacker's skills, which are specified in an attacker profile. The advantage of this approach is that it is possible to determine the ratio of cost to the attacker against the damage done to the bridge.

Table 1 provides information about each basic attack step leaf in the attack-fault tree segments in Figures 3 and 4. The w_1 and w_2 detection rates in the table are configured to be high (discussed later in the What-If scenario). The configuration assumes that detection occurs at a higher rate when an attacker is attempting to gain access but at a lower rate after access is gained. The attack labels and their categorizations as logical and physical attacks are relevant to the attack profiles.

The security analysis modeled the attacks in UPPAAL using the As-Is and What-If scenarios [16]. In the As-Is scenario, detection capabilities were eliminated to establish a baseline for a successful attack based on an attacker profile. In the What-If scenario, the w_1 and w_2 detection rates were set to high. This enabled the determination of the effectiveness of the detection mechanisms at preventing attacks.

5.2 Fault Leaf Automata

Exponential probability distributions with means λ are used to model the failure rates, where the probability of a failure at time t is $P(t) = 1 - e^{-\lambda t}$. A stochastic automaton is employed to simulate each basic component failure as described in [16]. Each automaton has a λ-value that expresses the exponential failure rate of the failing node (component). After a period of time, damage d occurs to the system, which transitions to the failed state and sends a message to a higher attack-fault tree gate that the component has failed. Each fault leaf in

Table 1. Basic attack step leaf information.

Attack	**Label**	**Path**	**Type**	**Description**
Cut Network	A_1	$[G_5] \rightarrow [G_6]$	Physical	$[G_5]$: $w_1 = 60$, $w_2 = 40$, $f = 20$, $v = 2$, $d = 5$, $\lambda = 0.0011$, $\lambda_1 = 0.0011$ $[G_6]$: $w_1 = 80$, $w_2 = 20$, $f = 5$, $v = 1$, $d = 50$, $\lambda = 0.00301$, $\lambda_1 = 0$
Jam Network Comms.	A_2	$[G_8] \rightarrow [G_9] \rightarrow [G_{11}]$	Logical	$[G_8]$: $w_1 = 60$, $w_2 = 40$, $f = 20$, $v = 2$, $d = 5$, $\lambda = 0.001188$, $\lambda_1 = 0.001188$ $[G_9]$: $w_1 = 60$, $w_2 = 40$, $f = 10$, $v = 1$, $d = 50$, $\lambda = 0.0011$, $\lambda_1 = 0.0011$ $[G_{11}]$: $w_1 = 80$, $w_2 = 20$, $f = 10$, $v = 1$, $d = 100$, $\lambda = 0.001$, $\lambda_1 = 0$
Inject Packets	A_3	$[G_8] \rightarrow [G_9] \rightarrow [G_{12}]$	Logical	$[G_{12}]$: $w_1 = 80$, $w_2 = 20$, $f = 30$, $v = 2$, $d = 250$, $\lambda = 0.001$, $\lambda_1 = 0$
Cut Power	A_4	$[G_{23}] \rightarrow [G_{24}]$	Physical	$[G_{23}]$: $w_1 = 60$, $w_2 = 40$, $f = 50$, $v = 3$, $d = 100$, $\lambda = 0.00092$, $\lambda_1 = 0.00092$ $[G_{24}]$: $w_1 = 80$, $w_2 = 20$, $f = 10$, $v = 2$, $d = 350$, $\lambda = 0.001$, $\lambda_1 = 0$
Stop Drive	A_5	$[G_{29}] \rightarrow [G_{30}]$	Logical	$[G_{29}]$: $w_1 = 60$, $w_2 = 40$, $f = 40$, $v = 3$, $d = 100$, $\lambda = 0.000596$, $\lambda_1 = 0.000596$ $[G_{30}]$: $w_1 = 80$, $w_2 = 20$, $f = 30$, $v = 2$, $d = 500$, $\lambda = 0.0005$, $\lambda_1 = 0$
Tamper with Brake	A_6	$[G_{29}] \rightarrow [G_{36}]$	Logical	$[G_{36}]$: $w_1 = 80$, $w_2 = 20$, $f = 40$, $v = 4$, $d = 500$, $\lambda = 0.0005$, $\lambda_1 = 0$
Stop Brake	A_7	$[G_{29}] \rightarrow [G_{37}]$	Logical	$[G_{37}]$: $w_1 = 80$, $w_2 = 20$, $f = 25$, $v = 2$, $d = 500$, $\lambda = 0.0005$, $\lambda_1 = 0$
Break Gear	A_8	$[G_{45}] \rightarrow [G_{46}]$	Physical	$[G_{45}]$: $w_1 = 60$, $w_2 = 40$, $f = 20$, $v = 4$, $d = 5$, $\lambda = 0.0011$, $\lambda_1 = 0.0011$ $[G_{46}]$: $w_1 = 80$, $w_2 = 20$, $f = 40$, $v = 8$, $d = 200$, $\lambda = 0.001092$, $\lambda_1 = 0$
Cause Explosion	A_9	$[G_{76}] \rightarrow [G_{77}]$	Physical	$[G_{76}]$: $w_1 = 65$, $w_2 = 35$, $f = 50$, $v = 4$, $d = 5$, $\lambda = 0.00037$, $\lambda_1 = 0.00037$ $[G_{77}]$: $w_1 = 80$, $w_2 = 20$, $f = 100$, $v = 10$, $d = 5000$, $\lambda = 0.000178$, $\lambda_1 = 0$

Figures 3 and 4 has its own automaton and the gates are stepped through during the UPPAAL simulation. Table 2 lists the sources of the λ-values corresponding to the basic component failures. All the failure rates are eventually expressed in terms of days so that the faults and attacks in the simulation have consistent time units. Note that the MTBF acronym in Table 2 denotes the mean time between failures.

Table 2. Basic component failure leaf sources and computation notes.

Failures	Source	Computation Notes
$[G_{15}], [G_{16}], [G_{17}]$	—	Assume MTBF is 20,000 hours based on a product review
$[G_{20}], [G_{33}]$	[11]	Assume annual failure rate is 0.4
$[G_{21}]$	[14]	Assume MTBF is 500 hours
$[G_{27}], [G_{38}]$	[20]	Assume failure rate is ten per million hours
$[G_{40}], [G_{42}], [G_{43}]$	[1]	Assume MTBF is 40,000 hours based on L10 life at the rated torque
$[G_{50}]$	[20]	Assume failure rate is eight per million hours at a 15-year renewal interval
$[G_{51}]$	[20]	Assume failure rate is 14 per million hours at a 15-year renewal interval
$[G_{53}]$	[20]	Assume failure rate is 20 per million hours at a 15-year renewal interval
$[G_{55}], [G_{57}], [G_{58}],$ $[G_{66}], [G_{67}], [G_{70}]$ $[G_{72}], [G_{73}], [G_{74}]$ $[G_{79}], [G_{80}]$	[6]	Assume or derive an annual failure rate
$[G_{60}], [G_{62}], [G_{63}]$	[8]	Assume failure rate is 1.09×10^{-7} per year based on concrete stress and corrosion data
$[G_{69}]$	—	Assume failure rate is 20 per million hours

6. Attack-Fault Tree Analysis

Simulations were conducted to quantify the impacts of attacks and faults on swing bridge operations. During each test, UPPAAL stepped through a number of runs until the results became statistically significant (or insignificant) to provide feedback on the results. A run was stopped and considered to be a hit if the goal $[G_0]$ was reached within a specified time frame. If the time expired before the goal $[G_0]$ was reached, then the run was considered to be a miss. Statistical significance was assessed using 95% confidence intervals.

6.1 Critical Fault Path Analysis

The first set of simulations was conducted to analyze the probability of disruption over time. Figure 6 shows the probabilities of disruption over time for five scenarios. This helps identify the paths that result in maximum disruption to the railroad bridge over a ten-year period. After one year, the Only Faults scenario yielded a fault probability $P(t \leq 365)$ of 0.75. After two years, the

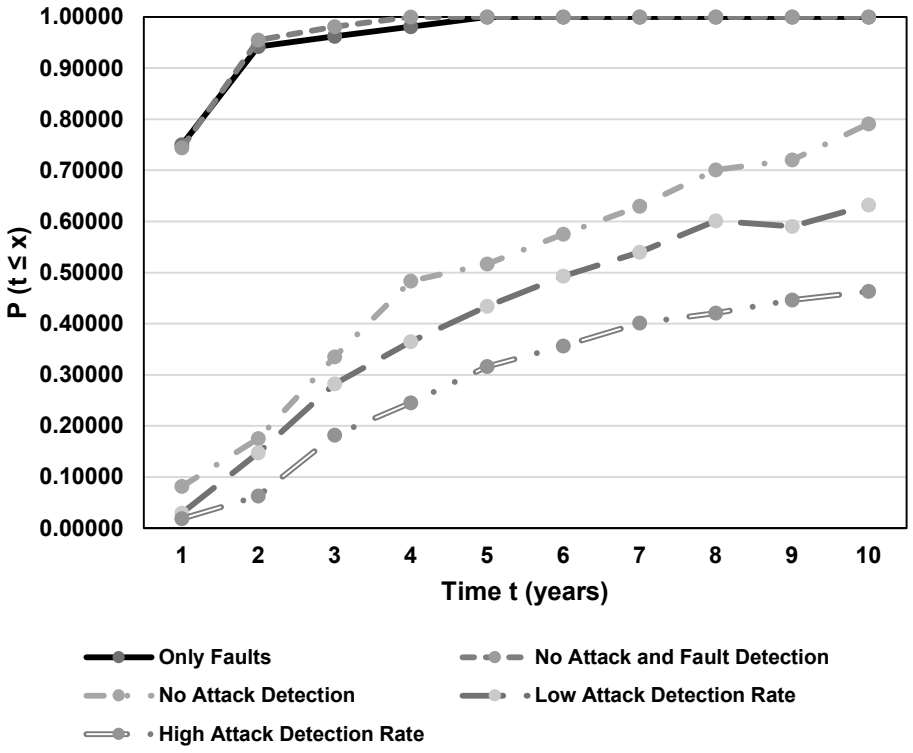


Figure 6. Probability of disruption at time t (95% confidence interval).

Only Faults scenario yielded a higher fault probability $P(t \leq 730)$ of 0.942. Scenarios with No Attack Detection, Low Attack Detection Rate and High Attack Detection Rate yielded two-year probabilities of 0.175, 0.147 and 0.0631, respectively.

The next set of simulations sought to identify the critical path in the attack-fault tree. This involved repeated simulations while disabling each basic component failure leaf in the attack-fault tree for a one-year period, where the Only Faults scenario yielded a fault probability $P(t \leq 365)$ of 0.75. After considering all the leaves, the percentage differences between the new results and the baseline value were computed.

Table 3 shows the results for all the basic component failure leaves. The results demonstrate that the power-related leaves pose the greatest risk to bridge failure. The G_{33} leaf corresponding to motor brake power failure yielded the greatest difference of -25.200% at $P(t \leq 365) = 0.561$, followed by G_{21} corresponding to generator failure with a difference of -21.730% and G_{20} corresponding to power outage with a difference of -19.870%. Note that G_{20} and G_{21} share the same critical failure path because the power generator should take

Table 3. Fault disruption percentages measured for all leaves (0.750).

Leaf	P(t ≤ 365)	Difference	Leaf	P(t ≤ 365)	Difference
G_{15}	0.720	–4.000%	G_{57}	0.748	–0.270%
G_{16}	0.693	–7.600%	G_{58}	0.734	–2.130%
G_{17}	0.724	–3.470%	G_{60}	0.749	–0.130%
G_{20}	0.601	–19.870%	G_{62}	0.716	–4.530%
G_{21}	0.587	–21.730%	G_{63}	0.748	–0.270%
G_{27}	0.702	–6.400%	G_{66}	0.758	1.070%
G_{33}	0.561	–25.200%	G_{67}	0.728	–2.930%
G_{38}	0.699	–6.800%	G_{69}	0.689	–8.130%
G_{40}	0.718	–4.270%	G_{70}	0.749	–0.130%
G_{42}	0.731	–2.530%	G_{72}	0.737	–1.730%
G_{43}	0.724	–3.470%	G_{73}	0.724	–3.470%
G_{50}	0.722	–3.730%	G_{74}	0.752	0.270%
G_{51}	0.708	–5.600%	G_{79}	0.722	–3.730%
G_{53}	0.697	–7.070%	G_{80}	0.735	–2.000%
G_{55}	0.735	–2.000%			

over in the event of a power failure. Generators are not built to last forever, but they have low exponential failure rates ($\lambda = 0.0042$). This may indicate a weakness in the model. Without some power system repair capabilities, the purpose of having a backup power system is defeated if its uptime (reliability) is less than the time between power failures.

6.2 Attacker Profile Analysis

Attacker profiles based on the attack-fault tree were created to evaluate various strategies against simulated adversaries. In particular, three attacker profiles were created to evaluate the effectiveness of adding security controls:

- **Nate:** Nation state attacker; Budget = $\$10,000 \times 10^3$; Success rate for logical attacks $p = 90\%$; Success rate for physical attacks $p = 90\%$.
- **Mallory:** Hacker; Budget = $\$5,000 \times 10^3$; Success rate for logical attacks $p = 80\%$; Success rate for physical attacks $p = 60\%$.
- **Chuck:** External attacker; Budget = $\$3,000 \times 10^3$; Success rate for logical attacks $p = 60\%$; Success rate for physical attacks $p = 80\%$.

Table 4 compares the results obtained for the As-Is and What-If scenarios by running the three attack profiles against the attack-fault tree over a ten-year time period.

In the As-Is scenario, Nate had a 36% chance of conducting a successful attack compared with 12.7% for Mallory and 10.2% for Chuck. Although Nate spent twice as much money on average in conducting a successful attack in

Table 4. As-Is versus What-If scenario results over ten years.

	Nate	**Mallory**	**Chuck**
As-Is Scenario			
Probability $P(t \leq 3,650)$	0.360	0.127	0.102
Mean Time E(t) (days)	828.469	606.163	410.418
Mean Cost E(cost) (10^3 dollars)	4,158.215	2,388.666	1,706.83
Mean Damage E(damage) (10^3 dollars)	1,066.595	1,058.763	442.77
Successful Attacks	133	22	14
Runs	371	182	150
What-If Scenario			
Probability $P(t \leq 3,650)$	0.226	0.0454	0.0515
Mean Time E(t) (days)	982.201	628.984	971.847
Mean Cost E(cost) (10^3 dollars)	4,409.470	1,650.969	1,776.107
Mean Damage E(damage) (10^3 dollars)	1,361.609	752.78	670.127
Successful Attacks	65	4	5
Runs	287	88	97

the average case as Mallory ($\$4,158.215 \times 10^3$ versus $\$2,388.666 \times 10^3$), they caused roughly the same amount of average damage per attack ($\$1,066.595 \times 10^3$ versus $\$1,058.763 \times 10^3$). This similarity suggests that logical attacks were likely to be more successful because Mallory had a higher probability of successful attacks. Meanwhile, Chuck spent an average of $\$1,706.83 \times 10^3$ per successful attack, resulting in an average of $\$442.77 \times 10^3$ in damage per successful attack. This also confirms that logical attacks are more likely to occur given the resources because Chuck is more likely to succeed with physical attacks. Time comparisons show that Nate (828.469 days) took longer on average than Mallory (606.163 days) and Chuck (410.418 days).

In the What-If scenario, the detection values for w_1 and w_2 were reconfigured as shown in Table 1. The percentages of successful attacks declined for Nate by –37.22%, Mallory by –64.25% and Chuck by –49.51%, demonstrating the utility of implementing detection mechanisms for all three attacker profiles. Nate's average time for attacks increased by 18.56% and cost increased by 6.04%, but he presumably took greater risks with his additional resources because the damage inflicted also increased by 27.66%. The simulation for Nate was executed ten additional times and similar results were obtained, confirming that the results were not anomalous. In contrast, Mallory saw an increase in the average time required to conduct successful attacks of only 3.76%, but decreases in cost of –30.88% and damage of –28.8%. Chuck saw a very large increase in the average time required to conduct successful attacks of 136.79%, only a slight increase in the average cost of 4.06%, but a large increase in damage of 51.35%. These results indicate that additional detection mechanisms would be more useful against strictly logical attackers (Mallory) than adversaries who are stronger at physical attacks (Nate and Chuck).

Table 5. Analysis of attack disruptions measured against $P(t \leq 3,650) = 0.341$.

Attack	$\mathbf{P(t \leq 3,650)}$	Difference	Attack	$\mathbf{P(t \leq 3,650)}$	Difference
A_1	0.275	–19.365%	A_6	0.347	1.858%
A_2	0.343	0.8072%	A_7	0.349	2.38%
A_3	0.343	0.8072%	A_8	0.358	5.234%
A_4	0.341	0%	A_9	0.339	–0.5234%
A_5	0.330	–3.244%			

6.3 Critical Attack Path Analysis

The observation that attackers with strengths in logical attacks may be at a disadvantage influenced the identification of critical attack paths in the attack-fault tree that might provide an explanation. This was accomplished by re-executing the No Attack Detection scenario discussed in Section 6.1 with Nate as the attacker.

The executions were configured to run for ten years without any detection mechanisms in place. After running through a baseline test with all the basic attack step leaves enabled, the differences in the new results with probability $P(t \leq 3,650) = 0.341$ were computed.

Table 5 shows the results for all the attack paths. The physical attack A_1, which physically cut network links, is critical because it has the highest difference: a –19.365% drop in the probability of successful attacks. This explains why physical attackers fared better in the What-If scenario. Upon applying detection methods of similar strength to both logical and physical attacks, adversaries who were stronger at physical attacks (Nate and Chuck) were still able to increase the amount of damage caused. This was due to their ability to perform attack A_1 that cut bridge network links with higher success rates.

7. Related Work

Previous work [27] introduced the security and safety risks facing movable railroad bridges and leveraged dynamic attack trees and fault trees to map possible vulnerabilities. Two separate models, one involving security and the other involving safety, were developed after researching control systems for a specific swing bridge. The previous work also revealed that many of the attacks and faults tended to overlap.

In contrast, the research described in this chapter integrates attacks and faults in a single model. The integrated attack-fault tree model was recently introduced by Kumar and Stoelinga [16], who used it to analyze a number of example systems. However, this chapter describes the first real-world application of the integrated attack-fault tree model, as well as the first application to a bridge system.

7.1 Historical Swing Bridge Failures

As discussed in the introductory section, data about swing bridge failures is limited due to a variety of factors. This research began by compiling data about swing bridge failures that was used to create the attack-fault tree.

The following additional information, categorized by the impacted swing bridge subsystems, is highly relevant to the faults considered in the model:

- **Superstructure System:** In 2014, a fire at a 104-year-old portal swing bridge in New York City cut power to the bridge. The resulting 70-minute outage delayed or cancelled 52 trains [17].

- **Substructure System:** The Gasparilla Island Swing Bridge in Charlotte County, Florida was recently replaced because its concrete girders from 1958 were structurally deteriorating, leading to high risks of failure due to storm surges and vehicular impacts [24]. Incident data about bridge allisions by marine vessels is posted by the U.S. Coast Guard [26].

- **Support System:** Older swing bridge center bearing designs are prone to instability when the bridges are unbalanced. As a result, a number of swing bridge renovation projects have been undertaken recently to address the problem, including the Court Street Bridge in Hackensack, New Jersey [3] and the East Haddam Swing Bridge in Connecticut [9]. In 2010, the Somerleyton Swing Bridge in Norfolk, England suffered a catastrophic failure due to a bearing system failure [22].

  Wedge faults have led to several prolonged swing bridge outages. In 2017, degraded wedges impacted operations of the Little Current Swing Bridge in Ontario, Canada [4]. In 2014, a complete wedge failure resulted in significant downtime of the Walk Bridge in Norwalk, Connecticut [23].

- **Drive System:** In 2010, a gearbox failure in the Whitby Swing Bridge in North Yorkshire, England terminated bridge operations for one week [2].

- **Interlocking System:** In 1996, Amtrak Train No. 12 derailed on the Portal Bridge near Secaucus, New Jersey due to defective miter rails $[G_{72}, G_{73}, G_{74}]$ [19]. In 2014, the Walk Bridge in Norwalk, Connecticut was closed due to an interlocking problem with its miter rails [23].

- **Electrical System:** An interesting story from 2002 about the Old Saybrook Bridge is recounted in [21]. This bascule bridge had electrical components dating back to its original design and construction in 1907. Troubleshooting the failed electrical system was an extremely complex task.

7.2 Rules and Regulations

Several rules and regulations govern the management of movable bridges in the United States. The U.S. Coast Guard oversees movable bridge operations

on navigable waterways. Organizations such as the American Association of Railroads (AAR) and the American Association of State Highway and Transportation Officials (AASHTO) promulgate national standards and requirements for movable bridge construction, maintenance and inspection. In addition, the following federal regulations govern movable bridge operations:

- **Movable Bridge, Interlocking of Signal Appliances with Bridge Devices (49 CFR 236.312 [12]):** This section specifies rules and restrictions governing the passage of trains over movable bridges.
- **Movable Bridge Locking (49 CFR 236.387 [13]):** This section mandates that movable bridges shall be inspected once a year.
- **Bridge Lighting and Other Signals (33 CFR Chapter 1, Sub-Chapter j, Part 118 [25]):** This section mandates the lighting requirements required for signaling the status of movable bridge operations on navigable waters.

8. Conclusions

Movable bridges have been used for hundreds of years, but they continue to evolve in their designs and implementations. Numerous movable bridges are being upgraded by automating and networking their components, which adds a new layer of risk to these vital transportation infrastructure assets. The research described in this chapter has leveraged the attack-fault tree model to integrate the physical risks involved in operating railroad swing bridges in the face of risks posed by physical attacks on bridge subsystems and cyber attacks on control systems.

The attack-fault tree approach integrates attacks and faults in a single model that supports the use of stochastic timed automata to identify the critical failure paths for a movable swing bridge. In particular, the integrated model reveals that physical network attacks and power faults are the best ways to disrupt movable swing bridge operations. Moreover, by stepping through the model, it was determined that superstructure and substructure system faults are statistical anomalies as far as the integrated attack-fault model is concerned. Thus, future research should focus on the attack surfaces and mechanical and electrical system failures.

The principal conclusion of this research is that the attack-fault tree approach is effective at identifying critical attack and fault paths at a high level. However, the swing bridge analysis reveals that the model falls short in some ways. In the case of a swing bridge, many faults can only occur only while the bridge is moving and other faults can occur only when the bridge is closed. The state of the system is, therefore, important, but the attack-fault tree model does not take the system state into account. For example, components such as electric motors and gears have failure rates that are established only when the system is in use. A movable bridge is in motion only for a few minutes at a time and these components spend the majority of their time at rest. Additionally,

the attack-fault tree allows for the incorporation of attack chains, but it does not necessarily consider the specific system configurations included in previous attack tree models. The attack-fault tree model also abstracts security control solutions as simple detection mechanisms, which reduces its applications in real-world environments.

Note that the views and opinions expressed herein are those of the authors and do not necessarily state or reflect the views and opinions of the Federal Railroad Administration or U.S. Department of Transportation, and shall not be used for advertising or product endorsement purposes.

Acknowledgements

This research was supported by Grant No. DTFR5317C00018 from the Federal Railroad Administration, U.S. Department of Transportation. The authors thank Mr. Francesco Bedini Jacobini and Mr. Jared Withers from the Federal Railroad Administration for their advice and assistance.

References

[1] G. Antony, How to determine the MTBF of gearboxes, *Power Transmission Engineering*, pp. 32–37, April 2008.

[2] BBC News, Swing bridge reopens in Whitby after gearbox failure, July 30, 2010.

[3] L. Burgos, Machinery rehabilitation of the Court Street Bridge over the Hackensack River, Hackensack, New Jersey, presented at the *Heavy Movable Structures Fourteenth Bienniel Symposium*, 2012.

[4] CBC News, Delays at swing bridge in Little Current due to repairs says MTO, July 7, 2017.

[5] P. Chaux, J. Roussel, J. Lesage, G. Deleuze and M. Bouissou, Towards a unified definition of minimal cut sequences, *Proceedings of the Fourth IFAC Workshop on Dependable Control of Discrete Systems*, paper no. 1, 2013.

[6] W. Cook, Bridge Failure Rates, Consequences and Predictive Trends, Ph.D. Dissertation, Department of Civil and Environmental Engineering, Utah State University, Logan, Utah, 2014.

[7] A. David, K. Larsen, A. Legay, M. Mikucionis and D. Poulsen, UPPAAL SMC tutorial, *International Journal on Software Tools for Technology Transfer*, vol. 17(4), pp. 397–415, 2015.

[8] C. Davis-McDaniel, Fault-Tree Model for Bridge Collapse Analysis, M.S. Thesis, Department of Civil Engineering, Clemson University, Clemson, South Carolina, 2011.

[9] J. DeWolf, History of Connecticut's Short-Term Strain Program for Evaluation of Steel Bridges, Report No. CT-2251-F-09-6, Connecticut Department of Transportation, Storrs, Connecticut, 2009.

[10] H. Douthit, The Use and Effectiveness of Sabotage as a Means of Unconventional Warfare – An Historical Perspective from World War I through Viet Nam, M.S. Thesis, School of Systems and Logistics, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 1987.

[11] R. Eacker and M. Bardsley, Electrical reliability analysis for transit applications, *Proceedings of the ASME/IEEE Joint Railroad Conference*, pp. 81–88, 2002.

[12] Federal Railroad Administration, Code of Federal Regulations, Title 49, Section 236.312 – Movable Bridge, Interlocking of Signal Appliances with Bridge Devices, Department of Transportation, Washington, DC, 2018.

[13] Federal Railroad Administration, Code of Federal Regulations, Title 49, Section 236.387 – Movable Bridge Locking, Department of Transportation, Washington, DC, 2018.

[14] G. Hansen, E. Frame and E. Sattler, Generator Set Durability Testing, Interim Report TFLRF No. 419, U.S. Army TARDEC Fuels and Lubricants Research Facility, Southwest Research Institute, San Antonio, Texas, 2012.

[15] T. Koglin, *Movable Bridge Engineering*, John Wiley and Sons, Hoboken, New Jersey, 2003.

[16] R. Kumar and M. Stoelinga, Quantitative security and safety analysis with attack-fault trees, *Proceedings of the Eighteenth IEEE International Symposium on High Assurance Systems Engineering*, pp. 25–32, 2017.

[17] P. McGeehan, 104-year-old portal bridge presents $900 million problem for rail commuters, *The New York Times*, September 25, 2014.

[18] S. Morgan, Burlington Northern Railroad Bridge 9.6, *Wikipedia* (`en.wikipedia.org/wiki/Burlington_Northern_Railroad_Bridge_9.6#/media/File:BNSF_Bridge_9.6_swing_span_turning.jpg`), June 25, 2011.

[19] National Transportation Safety Board, Derailment of Amtrak Train No. 12 and Sideswipe of Amtrak Train No. 79 on Portal Bridge near Secaucus, New Jersey, November 23, 1996, Railroad Special Investigation Report, Notation 6813B, Washington, DC, 1996.

[20] Naval Surface Warfare Center (Carderock Division), *Handbook of Reliability Prediction Procedures for Mechanical Equipment*, West Bethesda, Maryland, 2010.

[21] P. O'Neill and A. Ostrovsky, Failure and quick recovery of movable bridge on the Acela Line, presented at the *Heavy Movable Structures Ninth Biennial Movable Bridge Symposium*, 2002.

[22] M. Rimmer, Somerleyton Swing Bridge, Report by Waterways Strategy Officer, Navigation Committee, 2 September 2010, Agenda Item No. 8, Broads Authority, Norwich, United Kingdom, 2010.

[23] Short Term Action Team, Connecticut DOT BR. NO. 04288R Walk Bridge over Norwalk River, Norwalk, Connecticut, Emergency Repair and Reliability Report FINAL July 17, 2014, Connecticut Department of Transportation, Newington, Connecticut, 2014.

[24] H. Sinson, Gasparilla Island Swing Bridge replacement, presented at the *Heavy Movable Structures Sixteenth Biennial Movable Bridge Symposium*, 2016.

[25] United States Coast Guard, Code of Federal Regulations, Title 33 – Navigation and Navigable Waters, Washington, DC, 2010.

[26] United States Coast Guard, Homeport, Washington, DC (`homeport.uscg.mil`), 2019.

[27] Y. Wang, M. Jablonski, C. Yavvari, Z. Wang, X. Liu, K. Holt and D. Wijesekera, Safety and security analysis for movable railroad bridges, presented at the *ASME Joint Rail Conference*, 2019.